

#7

INFORMATION DISCLOSURE STATEMENT

BY APPLICANT

Docket: 245-53435

App:

Applicant: Çetin K. Koç, Erkey Savaş

Filed:

Art Unit:

JC682 U.S. PTO
09/558138
04/25/00

OTHER DOCUMENTS

B. S. Kaliski, Jr., "The Montgomery Inverse and Its Applications," IEEE Transactions on Computers 44:1064-1065 (August 1995)

P. L. Montgomery, "Modular Multiplication Without Trial Division," Mathematics of Computation 44:519-521 (April 1985)

Ç. K. Koç et al., "Analyzing and Comparing Montgomery Multiplication Algorithms," IEEE Micro 16:26-33 (June 1996)

J. Dhem et al., "SCALPS: Smart Card For Limited Payment Systems," IEEE Micro 16:42-51 (June 1996)

EXAMINER:

DATE:

*Examiner: Initial if considered, whether or not in conformance with MPEP 60;
draw line through cite if not in conformance and not considered. Send copy.

RECEIVED

JUL 11 2002

Technology Center 2600

Docket: 245-53435

App: 09/558,138

Applicant: Koc et al.

Filed: April 25, 2000

Art Unit: 2688

INFORMATION DISCLOSURE
STATEMENT

BY APPLICANT

OTHER DOCUMENTS

- | | | |
|--|-------------------------------------|---|
| | <input checked="" type="checkbox"/> | Menezes, et al., <u>Handbook of Applied Cryptography</u> , p. 600-603 (CRC Press 1997). |
| | <input checked="" type="checkbox"/> | S. Even, "Systolic Modular Multiplication," <u>Advances in Cryptology</u> , Lecture Notes in Computer Science 537 :619-624 (Springer Verlag 1990). |
| | <input checked="" type="checkbox"/> | Bosselaers et al., "Comparison of Three Modular Reduction Functions," <u>Crypto '93</u> , pp. 175-186 (1993). |
| | <input checked="" type="checkbox"/> | Koc et al., "Carry-save Adders for Computing the Products AB Modulo N," <u>Electronics Letters</u> 26 :899-900 (June 21, 1990). |
| | <input checked="" type="checkbox"/> | C.K. Koc., "Montgomery Reduction with Even Modulus," <u>IEEE Proc.-Compt. Digit Tech.</u> , 141 :314-316 (September 5, 1994). |
| | <input checked="" type="checkbox"/> | Paar et al., "Fast Arithmetic Architectures for Public-Key Algorithms over Galois Fields $GF((2^n)^m)$," <u>Eurocrypt '97</u> , p. 363-378 (May 11, 1997). |
| | <input checked="" type="checkbox"/> | Leu et al., "A Scalable Low-Complexity Digit-Serial VLSI Architecture for RSA Cryptosystem." <u>SiPS 99 IEEE Workshop on Signal Processing Systems</u> , p. 586-595 (1999). |
| | <input checked="" type="checkbox"/> | Bartee et al., "Computation with Finite Fields," <u>Information and Control</u> 6 :79-98 (1963). |
| | <input checked="" type="checkbox"/> | C.D. Walter, "Faster Modular Multiplication by Operand Scaling," <u>Advances in Cryptology: Lecture Notes in Computer Science</u> 576 :313-323 (1992). |
| | <input checked="" type="checkbox"/> | Bajard, et al., "An RNS Montgomery Modular Multiplication Algorithm," <u>IEEE Trans. on Computers</u> , 47 :766-776 (July 1998). |
| | <input checked="" type="checkbox"/> | Koc et al., "Montgomery Multiplication in $GF(2^k)$," <u>Designs, Codes and Cryptography</u> , 14 :57-69 (April 1998). |
| | <input checked="" type="checkbox"/> | G.B. Agnew et al., "Arithmetic Operations in $GF(2^m)$," <u>Journal of Cryptology</u> , p. 3-13 (1993). |

EXAMINER:

DATE

11-24-03

*Examiner: Initial if considered, whether or not in conformance with MPEP 609; draw line through cite if not in conformance and not considered. Send copy.